A Short Summary of Information Operations Terms

by Colonel Harry D. Tunnell IV

IO Sphere's Editor's Note: COL Tunnell has uncovered a basic truism in Information Operations and that is that there is no really good single source document to explain the simple terms of IO much less more complex practices. It is the lack of wide-spread common reference that makes IO such a tremendous challenge that requires true artist to successfully apply the elements in the war fight.

Introduction: Why is This Dialogue Necessary?

Information, and its use by the United States, is often touted as the only way to win the war of ideas with America's totalitarian terrorist enemies. If this assumption is taken at face value—that information is critical to success in this war—then audiences throughout the government ought to speak the same language whenever discussing approaches to apply this instrument of national power. Unfortunately, there is no single source for common IO terms.

Common understanding of many of the words and phrases that relate to information and its application to today's war is lacking. Definitions are taken directly from the private sector and modified for military or public use; military terms are often defined in joint and service literature—and all might be described differently; and now that information is highlighted as an essential component of America's warfighting strategy, new words are being developed to explain its use, and existing terminology is being modified as doctrine evolves.

This essay is an effort to collect the most commonly used terms in one place, define them, and provide a short reference for military and other government professionals. Since there are occasionally multiple meanings for the same phrases, this article relies on the explanations that are found in policy documents for political terms, joint doctrine for words unique to the armed forces, and NATO explanations for international military items.[2] If something is poorly defined or in developing doctrine then the document from the highest branch of government (or senior military headquarters) has been used; if more than one characterization is relevant to the conduct of military operations then all appropriate ideas are explained.

The Strategic Instruments.

Two concepts have direct strategic-level significance: information as an instrument of national power and strategic communication. The Reagan administration in National Security Decision Directive Number 130 defined information as a "key strategic instrument

Secretary of State Clinton in Haiti
Source: defenseimagery.mil

for shaping fundamental political and ideological trends around the globe on a long-term basis and ultimately affecting the behavior of governments."[3] President Reagan, as further expressed in his directive, believed that information should be a strategic instrument that serves American national policy rather than a lower-level tactical tool used in support of United States diplomacy.[4] Today, largely because of the concepts outlined in Reagan's directive, information is formally considered an instrument of national power along with diplomacy, military activity, and economic measures.

Strategic communication is one way that the information component of national power manifests itself in a practical and global sense. It is how the United States government can understand audiences, engage groups in a "dialogue of ideas," advise leaders on the publicopinion implications of certain policies, and influence audience attitudes and behavior.[5] Successful strategic communication frequently requires the establishment of liaison activities with

> ***What we're trying to do is influence others to understand that these thugs, these terrorists, are not out for anyone's good interest . . . .***
>
> ***. . . information and how it is passed and how people absorb it is critical.*** *1*
>
> ***General Peter Pace, Former Chairman Joint Chiefs of Staff***

public, non-governmental, and international media agencies.[6] Correspondingly, the strategic communication process creates, strengthens, or preserves conditions favorable for the advancement of American interests, policies, and objectives. The United States military, as part of this government-wide approach, participates in these activities in order to understand, inform, and influence relevant foreign audiences.[7]

Measures That Support Strategic Action.

Public diplomacy, public affairs, and ***information operations*** underpin the strategic implements and, with the exception of public affairs, are carried out by a particular department. Public diplomacy is traditionally the domain of the State Department and its purpose is to engage, inform, and influence foreign audiences.[8] In addition to press briefings and other traditional forums, public diplomacy includes non-traditional information events such as military-to-military programs, summits, and cultural exchanges. Almost anything that the government does outside of the United States is public diplomacy.

Public affairs (often called "PA") on the contrary, and as the federal government commonly employs it, is a tool to keep the American public informed.[9] The military definition of public affairs is more precise and is "those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense."[10] Unlike public diplomacy and IO, many government and private groups conduct some type of public affairs function.

Public affairs take a straightforward approach to the information presented—it must be truthful, timely, and as accurate as reasonably possible. This is necessary because the public affairs representatives who are charged with this type of outreach must maintain their credibility with the media and others who accept their input and actually present the desired information about the armed forces to the public. Public affairs is a "related capability" of IO which means that it should be coordinated and integrated with core and supporting IO capabilities without compromising its primary purpose and the rules under which it operates.[11]

Information Operations (sometimes referred to as "military information operations" or "IO") are the responsibility of the Department of Defense even though their conduct may involve cooperation with the others in interagency community or another agency may have a similar information role. IO is defined as "the integrated employment of the core capabilities of electronic warfare, computer network operations,

Exercise Balikatan 2009 Opening Ceremony, Republic of the Phillipines

Source: defenseimagery.mil

psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own."[12] (Supporting capabilities are those that are involved in the information environment and contribute to IO; it is best if they are integrated with the core capabilities, but they can serve other, more varied, purposes.)[13]

Uniquely Military Terminology.

Civil-Military Operations (CMO) are a related capability of IO. CMO is a Department of Defense term for "activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, and to consolidate and achieve operational US objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. CMO may be performed by designated civil affairs, by other military forces, or by a combination of civil affairs and other forces."[14]

Combat Camera is a supporting capability of IO and is a Department of Defense term for "the acquisition and utilization of still and motion imagery in support of combat, information, humanitarian, special forces, intelligence, reconnaissance, engineering, legal, public affairs, and other operations involving the Military Services."[15]

Computer Network Attack (CNA) consists of "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[16] Even though electronic attack can be used against a computer, it is not CNA because it relies on the electromagnetic spectrum while CNA relies on the data stream to execute an attack.[17]

Computer Network Defense (CND) is "actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks."[18]

Computer Network Exploitation (CNE) is "enabling operations and intelligence collection capabilities conducted through the

A US Navy Mark V Boat on a Training Operation
Source: defenseimagery.mil

use of computer networks to gather data from target or adversary automated information systems or networks."[19]

Computer Network Operations (CNO), one of five core capabilities of information operations, is a Department of Defense term for attacking, deceiving, degrading, disrupting, denying, exploiting and defending electronic information and infrastructure. CNO is "computer network attack, computer network defense, and related computer network exploitation enabling operations."[20]

Counterintelligence is a supporting capability of IO and is a Department of Defense term for "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."[22]

Defense Support to Public Diplomacy (DSPD), another related capability of IO, is a Department of Defense term for "those activities and measures taken by the Department of Defense components to support and facilitate

because IO planning is "an integral part of, not an addition to, the overall planning effort."[26]

Unfortunately, information campaign remains as much a part of the informal military lexicon as "air campaign," "land campaign," or "maritime campaign." Therefore, the topic merits further discussion. This still undefined term is sometimes used to describe a series of coordinated IO activities. Lieutenant Colonel Garry Beavers (USA, Ret.) in a Military Review article proposes the following definition: "offensive and defensive information operations that convey true, unclassified information about military operations and the information environment to external audiences."[27] Regrettably, Beavers allows Balkans-specific experiences to typify his concept of IO and therefore, the information campaign that he describes does not fully consider the information environment in which the Department of Defense operates during the Global War on Terrorism.

Any information campaign conducted by military forces, particularly during combat operations, should not be hindered by an artificial restriction such as to "convey true, unclassified information."

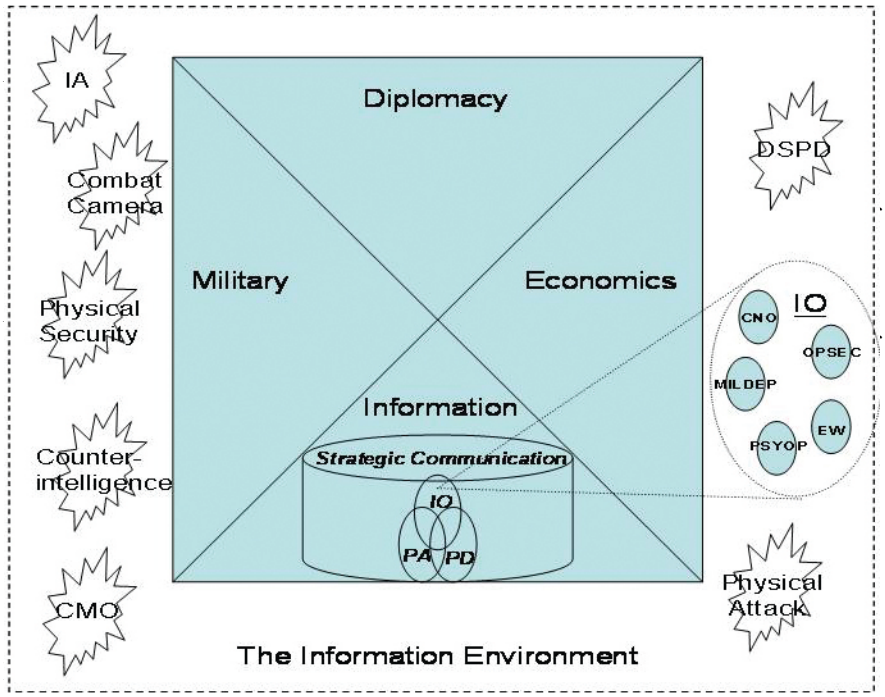

Figure: Relationships That Affect the Information Environment.

Information Superiority is a Department of Defense term for "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[28]

Military Deception (MILDEC), one of five core capabilities of information operations, is a Department of Defense term for "actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission."[29]

Operations Security (OPSEC), one of five core capabilities of IO, is a Department of Defense term for "a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation."[30]

Perception Management is generally associated with psychological operations. This term describes "actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning as well as to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations."[31]

Physical Attack is a Department of Defense term that describes another supporting capability of IO. "Physical attack disrupts, damages, or destroys adversary targets through destructive power. Physical attack can also be used to create or alter adversary perceptions or drive an adversary to use certain exploitable information systems."[31]

Physical Security is a supporting capability of IO and is a Department of Defense term for "that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. In communications security, the component that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons."[33]

Psychological Operations (PSYOP), one of five core capabilities of IO, is a Department of Defense term for "planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives."[34] (Note that the United States military use of the term limits psychological operations to target foreign audiences.)

Public Information is a Department of Defense term for "information of a military nature, the dissemination of which through public news media is not inconsistent with security, and the release of which is considered desirable or nonobjectionable to the responsible releasing agency."[35] United States military application of this term differs slightly from the NATO use of the term.

A Few International Terms.

Psychological Operations as used in NATO are "planned psychological activities in peace and war directed to enemy, friendly, and neutral audiences in order to influence attitudes and behavior affecting the achievement of political and military objectives. They include strategic psychological activities, psychological consolidation activities, and battlefield psychological activities."[36] This differs from its American counterpart.

Public Information as used in NATO describes, "Information which is released or published for the primary purpose of keeping the public fully informed, thereby gaining their understanding and support."[37] Again, this differs from its American counterpart.

Military, Government, and Private Sector Terms.

Biometrics is defined by the Committee on National Security Systems as "automated methods of authenticating or verifying an individual based upon a physical or behavioral characteristic."[38] Biometric technology is becoming an increasingly important part of government efforts during the Global War on Terrorism as a method to identify or categorize friendly and enemy personnel. Additional uses for this technology continue to develop, and its potential to influence activities in the information environment has not yet been fully realized.

Critical Infrastructure Protection (CIP), as defined by the Department of Defense, is "actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets."[39] There is another perspective on critical infrastructure protection that is important to military leaders because it relates to homeland security and homeland defense; this explanation is taken from a Presidential Executive Order.

NATO and Coalition Operations In Afghanistan
Source: defenseimagery.mil

Humanitarian Assessment Team and Host Nation Cooperation
Source: defenseimagery.mil

In his executive order, President Bush notes that the "information technology revolution" has caused business transactions, government operations, and national defense to depend on an interdependent network of critical information infrastructures. America's critical infrastructure protection program, therefore, must secure these infrastructures (including emergency preparedness communications and any associated supporting physical assets because protecting this is vital to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services sectors).[40]

Information Assurance (IA) is a supporting capability of IO and is a Department of Defense term for "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."[41] IA is listed in this section because it is a common term in both government and civilian use to describe comparable functions (with the exception of any relationship to IO).

Conclusion.

The reader should now understand there might be several variations for the same phrase or that some of the doctrinal definitions still need work. As the art of employing information at the strategic, operational, and tactical levels of war evolves, so must the language to describe what is happening throughout the information environment ("the aggregate of individuals, organizations, and systems that collect, process, or disseminate information"[42]). Until this unique "dialect" is refined and standardized, this commentary should serve as a useful tool for the beginner and old hand alike.

Footnotes:

1 ***Remarks to interviewer Jed Babbin on the Hugh Hewitt radio show, as cited in Jim Garamone, "Gen. Pace: Information is crucial in war on terror." Pentagram, October 28, 2005. On line version, http://www.dcmilitary.com/army/pentagram/10_43/national_news/37939-1.html, accessed January 26, 2006.***

2. For example there is a joint definition for electronic warfare but United States Air Force doctrine, while acknowledging the Joint Staff's definition, lists a "preferred" definition for the Air Force.

3. President Reagan, National Security Decision Directive Number 130: US International Information Policy (Washington, D.C.: U.S. Government, March 6, 1984), 1.

4. Summarized from ibid.

5. Paraphrased from the Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, Report of the Defense Science Board Task Force on Strategic Communication (Washington, D.C.: U.S. Government, September 2004), 11. The phrase, "dialogue of ideas," is a direct quote from page 11 of the report. The report is hereafter referred to as the DSB Report.

6. The DSB Report discusses what it identifies as four core instruments of Strategic Communication: Public Diplomacy, Public Affairs, International Broadcasting Services, and Information Operations. In the report International Broadcasting Services are organizations that are government funded and serve a variety of purposes. For the purpose of this essay International Broadcasting Services (as well as groups that perform similar functions) are included in the category of "public, non-governmental, and international media agencies."

7. Summarized from the Joint Staff, Joint Publication 3-13: Information Operations, Washington, D.C.: U.S. Government, 13 February 2006, I-10. Hereafter referred to as Joint Pub 3-13. The military, in Joint Pub 3-13, defines strategic communication as "focused USG [United States Government] efforts to understand and engage key audiences in order to create, strengthen or preserve conditions favorable for the advancement of USG interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all elements of national power." Even though the Joint Staff has defined strategic communication it is not responsible for America's strategic communication policy, process, or implementation and that is why the Joint Staff definition is not relied upon for this essay.

8. The definition for public diplomacy is paraphrased from the United States Department of State website, http://www.state.gov/r/, accessed July 26, 2005. The military, in the DOD Dictionary of Military and Associated Terms, as amended through August 31, 2005, defines it as "those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad."

9. It is difficult to pin down a precise definition of public affairs. The United States government generally considers public affairs to be a form of outreach to domestic American audiences although there are other audiences that public affairs affect. See DSB Report, 12 for a discussion of public affairs and the United States government.

10. DOD Dictionary of Military and Associated Terms, as amended through August 31, 2005, http://www.dtic.mil/doctrine/jel/doddict/index.html.

11. The idea of a related capability is paraphrased from Joint Pub 3-13, x. Civil-Military Operations and Defense Support to Public Diplomacy are also related capabilities.

12. Ibid., GL-9.

13. Paraphrased from ibid., x. Information assurance, physical security, physical attack, counterintelligence, and combat camera are considered the main supporting capabilities.

14. Ibid., GL-4.

15. Ibid., GL-5.

16. Ibid., GL-5.

17. Paraphrased from the DOD Dictionary.

18. Joint Pub 3-13, GL-5.

19. Ibid., GL-6.

20. Paraphrased from ibid., II-4 – II-5.

21. Ibid., GL-6.

22. Ibid., GL-6.

23. Ibid., GL-7.

24. DOD Dictionary.

25. Joint Pub 3-13, V-1.

26. Ibid.

27. Garry J. Beavers, Lieutenant Colonel (USA, Ret.), "Defining the Information Campaign," Military Review, November – December 2005, 80-82.

28. Joint Pub 3-13, GL-9.

29. DOD Dictionary.

30. Ibid.

31. Ibid.

32. Joint Pub 3-13, II-7.

33. Ibid., GL-11.

34. DOD Dictionary.

35. Ibid.

36. Ibid.

37. Ibid.

38. The Committee on National Security Systems, "CNSS Instruction No. 4009," National Information Assurance (IA) Glossary, revised May 2003, 6, website accessed 1-8 February 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf. The CNSS provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems operated by the US Government, its contractors, or agents.

39. DOD Dictionary.

40. Paraphrased from President Bush, Press Release: "Executive Order on Critical infrastructure Protection" (Washington DC: Office of the Press Secretary, October 16, 2001). Website accessed January 27, 2006, http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html. CNSS Instruction No. 4009, 18 specifically defines critical infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and government."

41. Joint Pub 3-13, GL-9 and CNSS Instruction No. 4009, 32.

42. Joint Pub 3-13, GL-9. Joint Pub 3-13, I-1 further notes that the "information environment is made up of three interrelated dimensions: physical, informational, and cognitive."

IO SPHERE

Joint Information Operations Warfare Center
JIOWC Mission Area Preparation Course

IO Core and Supporting Elements

IO Planning and Orders

Scenario Based Course

JIOWC Experienced Professionals as Mentors and Instructors

Two Weeks of Instruction

Open to Military, Government, and Government Contractor

Information Operations Awareness and Planners Training